

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»



ЗАТВЕРДЖУЮ

Ректор НТУ «ХПІ»

Євген СОКОЛ

« 28 » 03 2025 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»

першого (бакалаврського) рівня вищої освіти

за спеціальністю **257 – Управління інформаційною безпекою**

галузі знань **25 – Воєнні науки, національна безпека, безпека державного кордону**

кваліфікація **бакалавр з управління інформаційною безпекою**

ЗАТВЕРДЖЕНО

ВЧЕНОЮ РАДОЮ НТУ «ХПІ»

Голова вченої ради

 / Євген СОКОЛ

Протокол № 4

від « 28 » березня 2025 р.

Харків 2025 р.

ЛИСТ ПОГОДЖЕННЯ

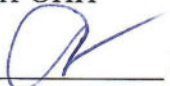
Освітньо-професійної програми Управління інформаційною безпекою

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	25 – Воєнні науки, національна безпека, безпека державного кордону
Спеціальність	257 «Управління інформаційною безпекою»
Кваліфікація	Бакалавр з управління інформаційною безпекою

СХВАЛЕНО

Робочою групою ОПП зі спеціальності
«Управління інформаційною безпекою»

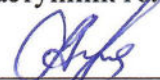
Гарант ОПП

 Роман КОРОЛЬОВ

Протокол № 1
« 26 » березня 2025 р.

РЕКОМЕНДОВАНО

Методичною радою НТУ «ХПІ»
Заступник голови методичної ради

 Руслан МИГУЩЕНКО

Протокол № 3
« 26 » березня 2025 р.

ПОГОДЖЕНО

Завідувач кафедри кібербезпеки

 Сергій ЄВСЕЄВ

Протокол № 12
« 14 » березня 2025 р.

ПОГОДЖЕНО

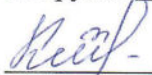
Директор навчально-наукового інституту
комп'ютерних наук та інформаційних
технологій

 Михайло ГОДЛЕВСЬКИЙ

« » 2025 р.

ПОГОДЖЕНО

Студент (член робочої групи ОПП)
№ групи КН-1423

 Артур КОНЮШЕНКО

« » 2025 р.

ЗАТВЕРДЖЕНО ТА НАДАНО ЧИННОСТІ

Наказом ректора Національного технічного університету «Харківський політехнічний інститут» від « 02 » квітня 2025 року № 111 ОД.

Ця освітньо-професійна програма не може бути повністю або частково відтворена, тиражована та розповсюджена без дозволу Національного технічного університету «Харківський політехнічний інститут».

РЕЦЕНЗЕНТИ:

Продуктивні зауваження та відгуки на проєкт освітньо-професійної програми одержано від:

1. Вадим МАШТАЛПР, доктор історичних наук, професор, заслужений винахідник України, начальник інституту інформаційно-комунікаційних технологій та кібероборони.
2. Юрій ПУНДА, доктор військових наук, старший науковий співробітник, начальник навчально-наукового центру підготовки офіцерів багатонаціональних штабів.
3. Валерій ШЕСТАКОВ, доктор технічних наук, доцент, лауреат Державної премії України в галузі науки і техніки, заступник директора (з навчальної та наукової роботи) Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України.
4. Сергій ГОЛОВАШИЧ, кандидат технічних наук, ТОВ “Мікрокрипт Текнолоджіс”, генеральний директор.



МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ УКРАЇНИ
ІМЕНІ ІВАНА ЧЕРНЯХОВСЬКОГО

Керівнику Національного технічного
університету "Харківський політехнічний
інститут"

Національний університет оборони України
імені Івана Черняхівського
03049, Київ, Повітрофлотський проспект 28.

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму "Управління інформаційною безпекою" бакалаврського (першого) рівня вищої освіти, що запропонована кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний."

Актуальність.

Стрімке зростання кількості кіберінцидентів, які стають все більш серйозними, призводить до необхідності підвищення безпеки, особливо у вразливій галузі, якою є критична інфраструктура. Однією з проблем безпеки критичних інфраструктур є рівень обізнаності про наслідки кібератак. Основною причиною ескалації кібератак у галузі критичної інфраструктури може бути те, що більшість систем управління, що використовуються для критичної інфраструктури, більше не використовують пропріетарні протоколи та програмне забезпечення, а використовують стандартні рішення. В результаті системи критично

важливої інфраструктури стають більш уразливими та схильними до кіберзагроз, ніж будь-коли раніше. Сучасний світ, фактично – це технології Індустрії 4.0 та Інтернету речей (Internet of Things), де фактичні ресурси мають свою віртуальну копію у цифровій формі та перехресшуються з традиційними підходами до документообігу та інформаційними системами супроводження безперервних бізнесів процесів. Це безумовно сприяє щорічному збільшенню попиту у нашій країні на спеціалістів з кібербезпеки, які будуть спроможні ефективно вирішувати складні завдання щодо побудови захисту підприємства та будуть спроможні забезпечувати протидію несанкціонованому втручання до їх інформаційної інфраструктури.

Характеристика програми.

Освітньо-професійна програма “УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ” першого бакалаврського рівня вищої освіти, що запропонована кафедрою кібербезпеки НТУ “ХП” має всі потрібні компоненти щодо забезпечення навчального процесу професійної підготовки фахівців, які у компаніях зможуть займати позиції: менеджера систем з інформаційної безпеки, адміністратора мереж і систем, фахівця з питань безпеки (інформаційно-комунікаційні технології), фахівця з підтримки інфраструктури кіберзахисту, фахівця з реагування на інциденти кібербезпеки тощо.

Слід визначити, що в умовах сучасних гібридних війн управління інформаційною безпекою – це не тільки значний тренд у розвитку великих компаній та підприємств, а також розвиток систем управління безпекою їх бізнес-процесів. Окремим питанням є формування можливості подальшого навчання щодо підготовки фахівців державних силових відомств. Це дозволяє формувати технічну складову майбутніх держслужбовців у галузі кібербезпеки та захисту інформації, а також окремо отримання поглиблених знань у сфері управління інформаційною безпекою. Тому, слід вважати дуже своєчасними завдання по формуванню професійних компетентностей,

що розглядаються в освітньо-професійній програмі “УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ”. Під час навчання студенти отримують фахові компетентності, які дозволять у майбутньому подальше навчання за спеціальностями у галузі як, інформаційна безпека, так й кібербезпека та захист інформації, як у державних закладах, так і в компаніях та підприємствах різних форм власності.

Висновок.

Слід підвести, що освітньо-професійна програма “УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ” бакалаврського (першого) рівня вищої освіти, що запропонована кафедрою кібербезпеки НТУ “ХПІ” є сучасною, ефективною та потрібною на ринку праці у нашої країни щодо підготовки фахівців з кібербезпеки та захисту інформації, з поглибленим вивченням питань, які пов’язані з управлінням інформаційною безпекою.

Відгук склав:

Начальник інституту інформаційно-комунікаційних технологій та кібероборони, заслужений винахідник України, доктор історичних наук, професор

14 березня 2024 року

Вадим МАШТАЛІР

Підпис заслуженого винахідника України, доктора історичних наук, професора Машталіра Вадима Віталійовича засвідчую:

Начальник адміністративного управління Національного університету оборони України імені Івана Черняховського



Богдан БІЛЯВСЬКИЙ



МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ УКРАЇНИ
ІМЕНІ ІВАНА ЧЕРНЯХОВСЬКОГО

Керівнику Національного технічного
університету "Харківський політехнічний
інститут"

Національний університет оборони України
імені Івана Черняхівського
03049, Київ, Повітрофлотський проспект 28.

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму "Управління інформаційною безпекою" бакалаврського (першого) рівня вищої освіти, що запропонована кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний."

Актуальність.

Стрімке зростання кількості кіберінцидентів, які стають все більш серйозними, призводить до необхідності підвищення безпеки, особливо у вразливій галузі, якою є критична інфраструктура. Однією з проблем безпеки критичних інфраструктур є рівень обізнаності про наслідки кібератак. Основною причиною ескалації кібератак у галузі критичної інфраструктури може бути те, що більшість систем управління, що використовуються для критичної інфраструктури, більше не використовують пропрієтарні протоколи та програмне забезпечення, а використовують стандартні рішення. В результаті системи критично

конкурентоспроможності у сучасних умовах. Звичайно, зараз наша країна потребує наявності кваліфікованих кадрів за напрямком “Управління інформаційною безпекою”.

Характеристика програми.

Слід відзначити високий рівень підготовки за запропонованою освітньо-професійною програмою, що поєднує навчання та опановування професійними компетентностями у галузі інформаційної/кібербезпеки та вивчення інформаційних технологій, особливостей програмування, набуття знань з іноземної мови та інші. Значна увага приділяється засвоєнню принципів, завдань системи управління інформаційною безпекою, вивченню нормативної та правової бази з питань організації та проведення аудиту інформаційної безпеки, методик оцінки інформаційних ризиків, здійсненню комплексу заходів, спрямованих на розроблення і впровадження інформаційних технологій, які забезпечують обробку інформації в інформаційно-телекомунікаційних системах згідно з вимогами, встановленими нормативно-правовими актами та нормативними документами у сфері захисту інформації.

Студенти, що навчаються за спеціальністю 257 “Управління інформаційною безпекою” мають можливість використовувати функціонал кіберполігону у якості практичної складової навчальної програми. Такий підхід, дозволяє студентам на реальних моделях поведінки зловмисників та сторони, що захищається від кібернападу, створювати окремі елементи системи управління інформаційної безпеки, опрацьовувати наближені до реальності події та бути здатними вже в умовах виробництва застосувати набуті знання та вміння в галузі управління інформаційною/кібербезпекою.

Висновок.

Вважаю, що освітньо-професійна програма “Управління інформаційною безпекою”, яка підготовлена кафедрою кібербезпеки НТУ “Харківський політехнічний інститут”, відповідає сучасним вимогам до підготовки фахівця за вищим освітнім рівнем бакалавр зі спеціальності 257 “Управління інформаційною безпекою”. Випускники цієї програми у разі досягнення очікуваних результатів навчання будуть спроможні забезпечувати інформаційну безпеку складних систем управління різного рівня та суб’єктності.

Відгук склав:

Начальник навчально-наукового центру підготовки офіцерів багатонаціональних штабів, доктор військових наук, старший науковий співробітник

Юрій ПУНДА

15 березня 2024 року

Підпис доктора військових наук, старшого наукового співробітника Пунди Юрія Васильовича засвідчую:

Начальник адміністративного управління Національного університету оборони України імені Івана Черняховського

Богдан БІЛЯВСЬКИЙ



РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму

“УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ”

бакалаврського (першого) рівня вищої освіти, яка запропонована

кафедрою кібербезпеки Національного технічного університету

“Харківський політехнічний інститут”

Відповідно до положень Стратегії інформаційної безпеки, яку затверджено Указом Президента України від 28.12.2021 №685/2021, забезпечення інформаційної безпеки України є однією з найважливіших функцій держави.

Протидія інформаційним впливам деструктивного характеру, насамперед держави-агресора, вимагає; створення системи раннього виявлення, прогнозування та запобігання інформаційним та гібридним загрозам. Кадрове забезпечення таких систем можливо здійснити фахівцями в галузі знань 25 Воєнні науки, національна безпека, безпека державного кордону за спеціальністю 257 Управління інформаційною безпекою.

Такі фахівці повинні бути компетентними в питаннях правового регулювання діяльності з управління інформаційною безпекою, застосуванні інформаційних технологій.

Освітня професійна програма “Управління інформаційною безпекою”, яка запропонована кафедрою кібербезпеки Національного технічного університету “Харківський політехнічний інститут” на рецензування, передбачає опановування професійними компетентностями з управління інформаційною безпекою. Її особливістю є планомірне та поступове вивчення спеціальних навчальних дисциплін щодо:

- нормативно-правової бази України, вимог відповідних міжнародних стандартів;

- алгоритмізації, програмування;

- застосування сучасних інформаційно-комунікаційних технологій;

- методів технічного захисту інформації, оцінювання рівня захищеності інформації;

- побудови та моделювання інформаційних систем;

- організації та ведення електронного документообігу, а також, документообігу з обмеженим доступом.

Освітньої професійна програма дозволить здобувачам вищої освіти оволодіти практичними навиками роботи з програмними системи розробки, забезпечення, моніторингу та контролю процесів інформаційної та/або кібербезпеки.

Вважаю, що освітньо-професійна програма, яка запропонована кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут", відповідає сучасним вимогам до підготовки фахівця за вищим освітнім рівнем бакалавр зі спеціальності 257 Управління інформаційною безпекою.

РЕЦЕНЗЕНТ

Заступник директора (з навчальної та наукової роботи) Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України, лауреат Державної премії України в галузі науки і техніки, доктор технічних наук, доцент

«27» 03 2023 року

Валерій ШЕСТАКОВ

Підпис Шестакова В. І. засвідчую.

Перший проректор (з навчальної роботи)
Національної академії Служби безпеки України
доктор юридичних наук, старший дослідник

«27» 03 2023 року

Віталій ГРЕБЕНЮК

ЗАТВЕРДЖУЮ:

Генеральний директор

ТОВ «Мікрокрипт Текнолоджіс»



«___»

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму “Управління інформаційною безпекою”
бакалаврського (першого) рівня вищої освіти, яка запропонована кафедрою
Кібербезпеки Національного технічного університету “Харківський
політехнічний інститут”

Стрімке проникнення автоматизації та інформаційних систем у всі без-
винятку галузі діяльності та комунікації сучасного суспільства нашої держави та
інших країн, також, неминуче тягне за собою і пов'язані ризики інформаційної
безпеки. Тому безпечне застосування інформаційних систем в сучасних умовах
неможливо без вирішення питань протидії кібернетичним загрозам, що існують
на різних рівнях організації суспільства: починаючи від критичної
інфраструктури держави, міністерств, відомств, органів державної влади та
самоуправління на місцях, великих галузеутворюючих підприємств та фінансових
установ, і до підприємств малого і середнього бізнесу. Саме тому комплексне
забезпечення інформаційної безпеки (ІБ) стала сьогодні невід'ємною функцією
будь-якої сучасної інформаційної системи, а ефективність застосування засобів
комплексної ІБ безпосередньо залежить від грамотного налагодження та
повсякденного керування, оновлення та постійної адаптації засобів ІБ до нових
загроз та методів вторгнення, що постійно еволюціонують. В зв'язку з цим,
підготовка висококваліфікованих фахівців з Управління інформаційною безпекою

є необхідною передумовою безпечної експлуатації інформаційних систем будь-якого масштабу.

Фахівці з Управління інформаційною безпекою повинні мати тверді знання сучасних принципів, методів та засобів як захисту інформації, так організації/виконання кібератак, яким вони мають протистояти в своїй роботі. Також, при підготовці фахівців цього профілю, особливу увагу слід приділяти вивченню: міжнародних та галузевих стандартів у сфері захисту інформації, криптографічних алгоритмів та протоколів, технічних засобів захисту, питанням розподілу повноважень та керування доступом, забезпеченню високого рівня надійності і доступності інформаційних систем. Обов'язковою умовою підготовки фахівців цього напрямку є надання студентам обширної інформації про сучасні засоби ІБ, представлені на ринку, та формування практичних навичок з оптимального вибору, конфігурування та застосування них для вирішення окремих задач кіберзахисту та побудови комплексної ІБ. Саме з метою досягнення перелічених вище цілей, кафедрою Кібербезпеки Національного технічного університету «Харківський політехнічний інститут» розроблено навчальну програму «Управління інформаційною безпекою». Навчальні плани та підбір дисциплін спрямовані на підготовку фахівців-практиків з кібербезпеки і надання їм теоретичних знань та формування практичних навичок, які передбачаються стандартом вищої освіти за спеціальністю 257 «Управління інформаційною безпекою».

Вважаю, що освітньо-професійна програма «Управління інформаційною безпекою», що розроблена та запропонована до впровадження кафедрою Кібербезпеки Національного технічного університету «Харківський політехнічний інститут», включає всі необхідні дисципліни в обсязі достатньому для підготовки кваліфікованих фахівців першого (бакалаврського) рівня освіти, які будуть мати великий попит на ринку праці.

Генеральний директор
ТОВ «Мікрокрипт Текнолоджис», к.т.н.



Головашич С.О.

ПЕРЕДМОВА

Відповідає галузі знань Воєнні науки, національна безпека, безпека державного кордону, спеціальності Управління інформаційною безпекою відповідно до національної рамки кваліфікації.

Розроблено робочою групою освітньо-професійної програми “Управління інформаційною безпекою”

Навчально-наукового інституту комп’ютерних наук та інформаційних технологій

Національного технічного університету “Харківський політехнічний інститут” у складі:

Гарант освітньо-професійної програми

Роман КОРОЛЬОВ, кандидат технічних наук, доцент кафедри кібербезпеки.

Члени робочої групи ОПП:

1. Сергій ЄВСЕЄВ, доктор технічних наук, професор, завідувач кафедри кібербезпеки.
2. Андрій ТКАЧОВ, кандидат технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки.
3. Артур КОНЮШЕНКО, студент групи КН-1423.

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ЗА СПЕЦІАЛЬНІСТЮ 257 – УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

1 – Загальна інформація	
Вищий навчальний заклад та структурний підрозділ	Національний технічний університет “Харківський політехнічний інститут”, Навчально-науковий інститут <u>комп’ютерних наук та інформаційних технологій</u> кафедра <u>кібербезпеки</u>
Ступінь вищої освіти та назва кваліфікації (освітньої, професійної) мовою оригіналу	Бакалавр Освітня кваліфікація: бакалавр з управління інформаційною безпекою. Кваліфікація в дипломі: бакалавр з управління інформаційною безпекою
Професійна кваліфікація	Відсутня
Форма навчання	Інституційна (очна (денна))
Офіційна назва освітньої програми	Управління інформаційною безпекою
Назва спеціалізації (предметних спеціальностей)	Відсутня
Тип диплому одиничний, спільний (подвійний) за наявності та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	Освітня програма ліцензована (на підставі наказу МОН України від 07.06.2024 № 394-л)
Цикл/рівень	Перший (бакалаврський) рівень вищої освіти, НРК – 6 рівень, EQF– 6 рівень, QF-EHEA – перший цикл.
Передумови	Для здобуття освітнього ступеня «бакалавр» можуть вступати особи, які здобули повну загальну середню освіту або освітній ступінь «молодший бакалавр», фаховий «молодший бакалавр», ОКР «молодший спеціаліст».
Мова викладання	Українська мова
Термін дії освітньо-професійної програми	Переглядається щорічно
Посилання на постійне розміщення опису освітньо-професійної програми	https://blogs.kpi.kharkov.ua/v2/quality/dokumenty/diyuchy-osvitni-programy/osvitnij-riven-bakalavr/
2 – Мета освітньо-професійної програми	
Надати освіту в сфері управління інформаційною безпекою для вирішення питань забезпечення виконання вимог міжнародних регуляторів та номативних	

законодавців актів країни щодо формування та використання системи управління інформаційною безпекою об'єктів критичної інфраструктури, широким доступом до працевлаштування (державні службовці органів державної влади та органів місцевого самоврядування, до сфери професійних обов'язків яких належить вирішення питань забезпечення безпеки життєдіяльності людини (індивіду), суспільства та держави, працівники недержавних та міжнародних організацій, науковоосвітніх установ, діяльність яких пов'язана із забезпеченням інформаційної безпеки) та створити передумови для подальшого вивчення державноуправлінських аспектів забезпечення безпеки на другому (магістерському) рівні вищої освіти.	
3 – Характеристика освітньо-професійної програми	
Предметна область (галузь знань, спеціальність, спеціалізація або предметна спеціальність (за наявності))	Галузь знань: 25 “Воєнні науки, національна безпека, безпека державного кордону” Спеціальність: 257 “Управління інформаційною безпекою” Об'єкт вивчення: – об'єкти систем управління інформаційною безпекою інформатизації, включаючи об'єкти критичної інфраструктури, кіберфізичні, соціокіберфізичні, інформаційні, інформаційно-аналітичні, інформаційно-комунікаційні системи; – технології забезпечення інформаційної безпеки; – процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Цілі навчання: підготовка фахівців здатних використовувати і впроваджувати технології управління інформаційною безпекою. Теоретичний зміст предметної області: Знання: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення системи управління інформаційною безпекою; – принципів супроводу систем та комплексів інформаційної безпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною безпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня інформаційної безпеки; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології управління інформаційною безпекою. Інструменти та обладнання: системи розробки, забезпечення, моніторингу та контролю процесів управління

	інформаційною безпекою; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; – спеціалізований клас (кіберполігон).
Орієнтація освітньої програми	Освітньо-професійна. Підготовка фахівців у сфері управління інформаційною безпекою
Основний фокус освітньої програми та спеціалізації або предметна спеціальність (за наявності)	Спеціальна освіта у галузі воєнних наук, національної безпеки, безпеки державного кордону зі спеціальності 257 “Управління інформаційною безпекою”. Спеціальна освіта за спеціальністю управління інформаційною безпекою, яка забезпечує підготовку професіонала, здатного розв’язувати задачі формування, використання, поліпшення системи управління інформаційною безпекою об’єктів критичної інфраструктури, кіберфізичних та соціокіберфізичних систем. Ключові слова: управління інформаційною безпекою, об’єкти критичної інфраструктури
Особливості програми	Особливістю програми спеціальності “Управління інформаційною безпекою” є проходження виробничої практики в органах державної влади, кіберполіції тривалістю 4 тижні.

**4 – Придатність випускників
до працевлаштування та академічні права випускників**

Придатність до працевлаштування	Фахівці з управління інформаційною безпекою можуть працювати, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010: 2139.2 Фахівець з криптографічного захисту інформації; 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології); 2139.2 Фахівець з підтримки інфраструктури кіберзахисту; 2139.2 Фахівець з реагування на інциденти кібербезпеки; 2139.2 Фахівець сфери захисту інформації; 2419.3 Радник (органи державної влади, місцевого самоврядування); 3411 Фахівець з фінансово-економічної безпеки; 3439 Фахівець з режиму секретності; 3439 Фахівець із організації захисту інформації з обмеженим доступом; 3439 Фахівець із організації інформаційної безпеки.
Академічні права випускників	Особа, яка закінчила навчання за цією освітньо-професійною програмою та здобула ступінь бакалавра може продовжити навчання на другому (магістерському) рівні вищої освіти (при проходженні відбору у національній академії СБУ), а також має можливість набуття додаткових кваліфікацій в системі післядипломної освіти та підвищення кваліфікації.

5 – Викладання та оцінювання	
Викладання та навчання	Студенто-центриське навчання, самонавчання, проблемно-орієнтоване навчання, навчання через практикуми, які відбуваються на базах практики. На другому і третьому курсі студенти пишуть та захищають курсові роботи, зорієнтовані на засвоєння ними теоретичних знань та вирішення управлінських спеціалізованих завдань у сфері національної безпеки. Під час останнього року навчання студенти пишуть кваліфікаційну (бакалаврську) роботу, яка також презентується та обговорюється за участю викладачів, одногрупників та рецензується зовнішнім рецензентом
Оцінювання	Письмові та усні іспити, диференційовані заліки, семінари, наукові звіти, есе, аналітичні записки, презентації самостійних досліджень, поточний контроль, контрольні роботи, курсові роботи, комплексний кваліфікаційний іспит, захист кваліфікаційної (бакалаврської) роботи за участі науковців з інших університетів. Оцінювання здійснюється за національною шкалою (“відмінно”, “добре”, “задовільно”, “незадовільно”), 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F).
6 – Програмні компетентності	
Інтегральна компетентність	Здатність здійснювати управлінську та проектну діяльність у визначені напрямів забезпечення захисту на об’єктах критичної інфраструктури, визначення політики та стратегії захисту інформації з обмеженим доступом, що передбачає застосування теорій та наукових методів у галузі управління інформацією безпекою
Загальні компетентності	ЗК1. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ЗК2. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. ЗК3. Здатність до абстрактного мислення, аналізу та синтезу. ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК5. Здатність спілкуватися іноземною мовою. ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК7. Здатність використовувати інформаційні та

	комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою. ЗК8. Здатність до соціальної взаємодії, співробітництва, розв'язання конфліктів у сфері професійної діяльності, лідерства і командної роботи.
Спеціальні (фахові) компетентності	СК1. Здатність використовувати безпекові режими під час виконання службових обов'язків. СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації. СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації. СК4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації. СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою. СК6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами. СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації. СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах. СК9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах. СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки. СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.
7 – Результати навчання	
Результати навчання за спеціальністю	РН1. Вміти реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства (вільного демократичного) та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні. РН2. Вміти використовувати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. РН3. Вміти за допомогою абстрактного мислення, аналізу та

	синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань. RH4. Вільно спілкуватися державною мовою. RH5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності. RH6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки. RH7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою. RH8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки. RH9. Вміти використовувати безпекові режими під час виконання службових обов'язків. RH10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки. RH11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків. RH12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. RH-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах. RH14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки. RH15. Вміти визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки. RH16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах. RH17. Вміти розв'язувати задачі управління інформаційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою. RH18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки
--	---

	документів, їх правильного використання в управлінській діяльності. РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах. РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки. РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем. РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідає кадровим вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова Кабінету Міністрів України “Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти” від 30 грудня 2015 р. № 1187, зі змінами, внесеними згідно з Постановою КМУ № 365 від 24.03.2021. Додаток 15-16). Склад робочої групи освітньої програми, професорсько викладацький склад, що задіяний до викладання навчальних дисциплін за спеціальністю відповідають Ліцензійним умовам провадження освітньої діяльності на першому (бакалаврському) рівні вищої освіти. До викладання залучаються викладачі-практики, фахівці та співробітники ІТ-компаній, а також фахівці Інституту СБУ, кіберполіції.
Матеріально-технічне забезпечення	Відповідає технологічним вимогам щодо матеріально-технічного забезпечення освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова кабінету міністрів України “Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти” від 30 грудня 2015 р., № 1187, зі змінами, внесеними згідно з Постановою КМУ № 365 від 24.03.2021. Додаток 17). Навчально-науково-виробнича база у вигляді: –навчальні корпуси, комп'ютерні класи, об'єднані локальною обчислювальною мережею з виходом до Інтернету, мультимедійне обладнання;–спеціалізоване програмне забезпечення; –бібліотека; гуртожитки; спортивні зали, майданчики; пункти харчування.
Інформаційне та навчально-	Інформаційне та навчально-методичне забезпечення освітньої програми відповідає постанові Кабінету

методичне забезпечення	Міністрів України від 30.12.2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» (зі змінами, внесеними згідно з Постановою КМ № 365 від 24.03.2021. Додаток 18). Інформаційне та навчально-методичне забезпечення навчального процесу реалізується наявністю необхідної навчальної та методичної літератури: підручники, навчальні посібники, методичні рекомендації до практичних занять, самостійної роботи, силабуси освітніх компонентів (https://cybersecurity.kpi.kharkov.ua/sylabusy-osvitnikh-komponentiv-257-bakalavr/). Інформаційні ресурси розміщені у фондах наукової бібліотеки НТУ «ХПІ», сайтах випускових кафедр. У навчальному процесі застосовується LMS (Learning Management System).
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів про академічну мобільність з університетами України. Меморандуму про співпрацю щодо реалізації програм внутрішньої академічної мобільності здобувачів вищої освіти за освітньою програмою “Кібербезпека” спеціальності 125 “Кібербезпека та захист інформації” з національною академією СБУ.
Міжнародна кредитна мобільність	На основі двосторонніх договорів
Навчання іноземних здобувачів вищої освіти	Підготовка іноземних громадян здійснюється згідно з вимогами чинного законодавства за умови визнання попереднього освітнього рівня.

2. ПЕРЕЛІК ОСВІТНІХ КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ» ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1 Перелік компонент освітньо-професійної програми

Код н/д	Компоненти освітньо-професійної програми	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. Обов'язкові освітні компоненти ОПП			
1.1 Загальна підготовка			
ЗП 1	Історія та культура України	4,0	Екзамен
ЗП 2	Українська мова (професійного спрямування)	3,0	Залік
ЗП 3	Іноземна мова	16,0	Залік, Екзамен
ЗП 4	Вища математика	12,0	Залік, Екзамен
ЗП 5	Основи гуманітарно-філософських знань у професійній діяльності	4,0	Екзамен
ЗП	Фізичне виховання	4,0	Залік
1.2 Спеціальна (фахова) підготовка			
СП 1	Вступ до спеціальності. Ознайомча практика	3,0	Залік
СП 2	Основи програмування	4,0	Екзамен
СП 3	Інформаційна безпека держави	6,0	Екзамен
СП 4	Теорія інформації і кодування	3,0	Екзамен
СП 5	Фізичні основи технічних засобів розвідки	5,0	Екзамен
СП 6	Алгоритми та структури даних	5,0	Екзамен
СП 7	Правове регулювання кібербезпеки	4,0	Залік
СП 8	Менеджмент інформаційної безпеки	3,0	Екзамен
СП 9	Технології програмування	5,0	Екзамен
СП 10	Математичні основи криптології	4,0	Екзамен
СП 11	Основи соціальної інженерії	4,0	Залік
СП 12	Комп'ютерні мережі	4,0	Екзамен
СП 13	Інструментальні засоби програмування	6,0	Екзамен
СП 14	Основи криптографічного захисту	6,0	Залік
СП 15	Цифрова криміналістика	6,0	Залік
СП 16	Моделювання інформаційних систем	4,0	Залік
СП 17	Організація документообігу з обмеженим доступом	5,0	Залік
СП 18	Інтернетика. Теорія пошуку. Моделі та алгоритми	4,0	Екзамен
СП 19	Безпека в інформаційно-комунікаційних системах	4,0	Залік
СП 20	Розробка веб-додатків	6,0	Екзамен
СП 21	Веббезпека	5,0	Залік
СП 22	Блокчейн та смарт-технології в електронному документообігу	4,0	Екзамен
СП 23	Безпека інтернет-речей	4,0	Залік
СП 24	Антивірусний захист інформації	5,0	Залік

1	2	3	4
СП 25	Гібридні війни та національна безпека	4,0	Залік
СП 26	Інтернет-розвідка	4,0	Екзамен
2. Практична підготовка			
ПП 5	Виробнича практика	6,0	Залік
ПП 6	Переддипломна практика	6,0	Залік
3. Атестація			
	Атестація	3,0	
Загальний обсяг обов'язкових компонент		175	
4. Вибіркові освітні компоненти ОПП			
4.1. Профільна підготовка			
4.1.1 Профільований пакет освітніх компонент 01 "Штучний інтелект в системах захисту"			
ВП1.1	Етичний хакінг	3,0	Екзамен
ВП1.2	Дата майнинг	3,0	Екзамен
ВП1.3	Математичні основи штучного інтелекту	3,0	Екзамен
ВП1.4	Python для штучного інтелекту та машинного навчання	4,0	Екзамен
ВП1.5	Генетичні алгоритми	3,0	Екзамен
ВП1.6	Python для інтернет-речей	3,0	Екзамен
ВП1.7	Системний інжиніринг	3,0	Екзамен
4.1.2 Профільований пакет освітніх компонент 02 "Блокчейн-технологія та безпека банківських систем"			
ВП2.1	Децентралізовані системи	3,0	Екзамен
ВП2.2	Ризик-менеджмент	3,0	Екзамен
ВП2.3	Blockchain: основи та приклади застосування	3,0	Екзамен
ВП2.4	Безпека банківських систем	4,0	Екзамен
ВП2.5	Захист об'єктів критичної інфраструктури	3,0	Екзамен
ВП2.6	Організація документообігу з обмеженням доступом	3,0	Екзамен
ВП2.7	Безпека в соціальних мережах	3,0	Екзамен
4.1.3 Профільований пакет освітніх компонент 03 "Innovation Campus"			
ВП3.1	Основи кібербезпеки	3,0	Екзамен
ВП3.2	Розробка корпоративних інформаційних систем (частина 1)	3,0	Екзамен
ВП3.3	Розробка корпоративних інформаційних систем (частина 2)	3,0	Екзамен
ВП3.4	Бази даних для корпоративних інформаційних систем	4,0	Екзамен
ВП3.5	Архітектура корпоративних інформаційних систем	3,0	Екзамен
ВП3.6	Безпека та аудит бездротових та рухомих мереж	3,0	Екзамен
ВП3.7	Захист об'єктів критичної інфраструктури	3,0	Екзамен
4. 2 Освітні компоненти вільного вибору професійної підготовки			

<i>загальноінститутського каталогу</i>			
<i>ОКВП 1</i>	<i>ОК ВВ ПП 1</i>	<i>4,0</i>	<i>Залік</i>
<i>ОКВП 2</i>	<i>ОК ВВ ПП 2</i>	<i>4,0</i>	<i>Залік</i>
<i>ОКВП 3</i>	<i>ОК ВВ ПП 3</i>	<i>4,0</i>	<i>Залік</i>
<i>ОКВП 4</i>	<i>ОК ВВ ПП 4</i>	<i>4,0</i>	<i>Залік</i>
<i>ОКВП 5</i>	<i>ОК ВВ ПП 5</i>	<i>4,0</i>	<i>Залік</i>
<i>ОКВП 6</i>	<i>ОК ВВ ПП 6</i>	<i>4,0</i>	<i>Залік</i>
<i>ОКВП 7</i>	<i>ОК ВВ ПП 7</i>	<i>4,0</i>	<i>Залік</i>
<i>4.3 Освітні компоненти вільного вибору загальноуніверситетського каталогу</i>			
<i>ОКВЗ 1</i>	<i>ОК ВВ ЗК 1</i>	<i>4,0</i>	<i>Залік</i>
<i>ОКВЗ 2</i>	<i>ОК ВВ ЗК 2</i>	<i>4,0</i>	<i>Залік</i>
<i>ОКВЗ 3</i>	<i>ОК ВВ ЗК 3</i>	<i>4,0</i>	<i>Залік</i>
<i>4.4 Освітні компоненти спеціального вибору університету</i>			
<i>ОКСВУ 1</i>	<i>ОКСВУ 1</i>	<i>3,0</i>	<i>Залік</i>
<i>ОКСВУ 2</i>	<i>ОКСВУ 2</i>	<i>3,0</i>	<i>Залік</i>
<i>Загальний обсяг вибіркових компонент:</i>		<i>68</i>	
<i>ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ:</i>		<i>240</i>	

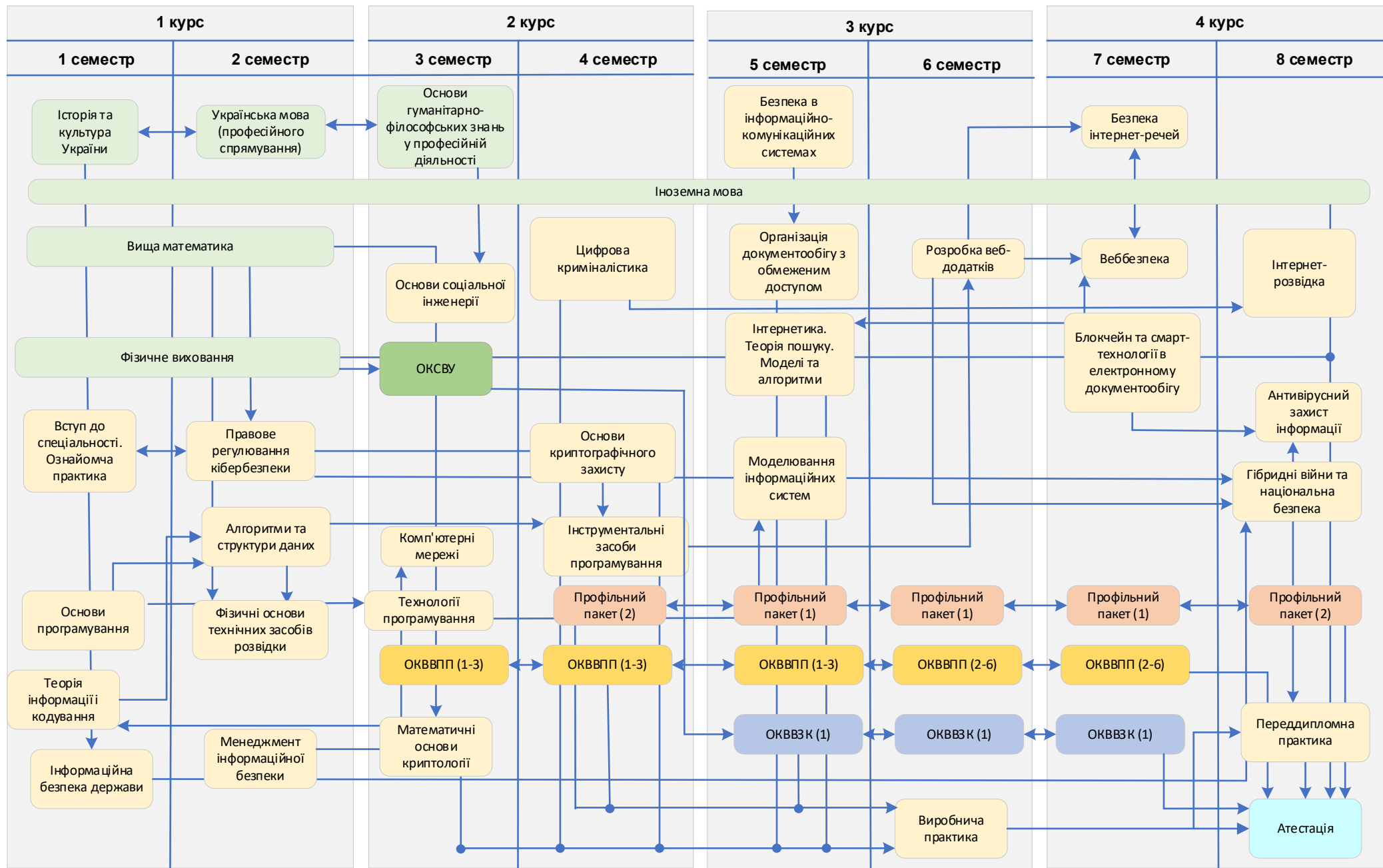
3. РОЗПОДІЛ ЗМІСТУ ОСВІТНЬОЇ ПРОГРАМИ ЗА ГРУПАМИ КОМПОНЕНТІВ ТА ЦИКЛАМИ ПІДГОТОВКИ

№ п/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів ECTS / %)		
		Обов'язкові компоненти освітньо-професійної програми	Вибіркові компоненти освітньо-професійної програми	Всього за весь термін навчання
1	Загальна підготовка	43 / 17,92	-	43 / 17,92
2	Спеціальна (фахова) підготовка	132/ 55	-	132/ 55
3	Компоненти вільного вибору	-	65 / 27,08	65 / 27,08
Всього за весь термін навчання		175 / 72,92	65 / 27,08	240 / 100

4. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційного проекту/роботи. На атестацію допускаються студенти, які виконали всі вимоги програми підготовки
Вимоги до кваліфікаційного проекту/роботи	Кваліфікаційний проект/робота має передбачати розв'язання спеціалізованої задачі в сфері кіберзахисту галузі національної безпеки. Кваліфікаційний проект/робота має бути перевірений на академічний плагіат та має бути оприлюднений (за виключенням робіт, що містять інформацію з обмеженим доступом) на офіційному сайті закладу вищої освіти або його структурного підрозділу, або у репозитарії закладу вищої освіти.

5. СТРУКТУРНО-ЛОГІЧНА СХЕМА



6. МАТРИЦЯ ВІДПОВІДНОСТІ ВИЗНАЧЕНИХ СТАНДАРТОМ КОМПЕТЕНТНОСТЕЙ / РЕЗУЛЬТАТІВ НАВЧАННЯ ДЕСКРИПТОРАМ НРК

Класифікація компетентностей (результатів навчання) за НРК	Знання Зн1. Концептуальні наукові та практичні знання. Зн2. Критичне осмислення теорій, принципів, методів і понять у сфері професійної діяльності та/або навчання	Уміння Ум1. Поглиблені когнітивні та практичні уміння/навички, майстерність та інноваційність на рівні, необхідному для розв'язання складних спеціалізованих задач і практичних проблем у сфері професійної діяльності або навчання.	Комунікація К1. Донесення до фахівців і нефахівців інформації, ідей, проблем, рішень власного досвіду та аргументації. К2. Збір, інтерпретація та застосування даних. К3. Спілкування з професійних питань, у тому числі іноземною мовою	Відповідальність і автономія АВ1. Управління складною технічною або професійною діяльністю чи проектами. АВ2. Спроможність нести відповідальність за вироблення та ухвалення рішень у непередбачуваних робочих та/або навчальних контекстах. АВ3. Формування суджень, що враховують соціальні, наукові та етичні аспекти. АВ4. Організація та керівництво професійним розвитком осіб та груп. АВ5. Здатність продовжувати навчання із значним ступенем автономії.
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
ЗК1	+	+	+	+
ЗК2	+	+	+	+
ЗК3	+	+		+
ЗК4	+	+	+	+
ЗК5	+	+	+	+
ЗК6	+	+		+
ЗК7	+	+		
ЗК8		+	+	
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
СК1	+	+		+
СК2	+	+		+
СК3	+	+		+
СК4	+	+		
СК5	+	+	+	+
СК6	+	+		+
СК7	+	+		+
СК8	+			
СК9	+	+	+	+
СК10	+	+		
СК11	+	+		

7. МАТРИЦЯ ВІДПОВІДНОСТІ ВИЗНАЧЕНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ, КОМПЕТЕНТНОСТЕЙ ТА ОСВІТНІХ КОМПОНЕНТІВ

[illegible]

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
			СП21 СП22 СП23 СП24 СП25 СП26 ПП5 ПП6			СП19 СП20 СП21 СП22 СП23 СП24 СП25 СП26 ПП6	СП23 СП24 ПП6												
PH4				ЗП2 ЗП5 ЗП СП3 СП4 СП5 СП7 СП8 СП12 СП13 СП14 СП17 СП18 СП19 СП20 СП22 СП23 СП24 СП25 СП26 ПП5 ПП6				ЗП2 ЗП3 ЗП5 ЗП СП1 СП5 СП7 СП17 ПП6											
PH5					ЗП3 СП3 СП5 СП8 СП12 СП13 СП14 СП18			ЗП2 ЗП3 ЗП5 ЗП СП1 СП5 СП7 СП17						СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19					

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
					СП19 СП22 СП23 ПП5 ПП6			ПП6						СП22 СП23 ПП6					
PH6							СП1 СП2 СП3 СП5 СП6 СП8 СП9 СП10 СП12 СП13 СП14 СП15 СП16 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП6		СП2 СП4 СП5 СП6 СП9 СП18 СП21 СП23 СП24 ПП5 ПП6	СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 СП26 ПП5 ПП6									
PH7							СП1 СП2 СП3 СП5 СП6 СП8 СП9 СП10 СП12		СП2 СП4 СП5 СП6 СП9 СП18 СП21 СП23 СП24	СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11									

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
							СП13 СП14 СП15 СП16 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП6		ПП5 ПП6		СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП5 ПП6								
PH8											СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП5 ПП6								
PH9									СП2 СП4 СП5 СП6 СП9 СП18										

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
									СП21 СП23 СП24 ПП5 ПП6										
PH10										СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 СП26 ПП5 ПП6	СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП5 ПП6								
PH11											СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11								

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
											СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП5 ПП6								
PH12											СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП5 ПП6								
PH13											СП3 СП4 СП5 СП7 СП11 СП17	СП3 СП4 СП5 СП8 СП9 СП11		СП1 СП4 СП5 СП8 СП12 СП13		СП3 СП4 СП5 СП8 СП9 СП12			

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
												СП20 ПП5 ПП6	СП12 СП13 СП14 СП15 СП18 СП19 СП22 СП23 СП24 ПП6		СП14 СП18 СП19 СП20 СП22 СП23 СП24 ПП5 ПП6		СП14 СП19 СП22 ПП6		
PH14																	СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ПП6	СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП18 СП19 СП21 СП22 СП23 ПП5 ПП6	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП22 СП23 ПП5 ПП6
PH15								ЗП2 ЗП3 ЗП5 ЗП СП1 СП5 СП7 СП17 ПП6											
PH16											СП1 СП2 СП4 СП5 СП6 СП8 СП9					СП1 СП3 СП4 СП5 СП8 СП10 СП11			

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
											СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП5 ПП6					СП12 СП14 СП16 СП19 СП20 СП22 ПП5 ПП6			
PH17											СП1 СП2 СП4 СП5 СП7 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП5 ПП6	СП3 СП4 СП5 СП7 СП11 СП17 СП20 ПП5 ПП6	СП3 СП4 СП5 СП8 СП9 СП11 СП12 СП13 СП14 СП15 СП18 СП19 СП22 СП23 СП24 ПП6			СП1 СП3 СП4 СП5 СП8 СП9 СП10 СП11 СП12 СП14 СП16 СП19 СП20 СП22 ПП5 ПП6		СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП18 СП19 СП22 ПП6	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22 СП23 ПП5 ПП6
PH18							СП1 СП2 СП3 СП5		СП2 СП4 СП5 СП6		СП1 СП2 СП4 СП5	СП3 СП4 СП5 СП7	СП3 СП4 СП5 СП8	СП4 СП5 СП8 СП12					

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
							СП6 СП8 СП9 СП10 СП12 СП13 СП14 СП15 СП16 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП6		СП9 СП18 СП21 СП23 СП24 ПП5 ПП6		СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП5 ПП6		СП11 СП17 СП20 ПП5 ПП6	СП9 СП11 СП12 СП13 СП14 СП15 СП18 СП19 СП22 СП23 СП24 ПП6					
PH19							СП1 СП2 СП3 СП5 СП6 СП8 СП9 СП10 СП12 СП13 СП14 СП15 СП16 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП6		СП2 СП4 СП5 СП6 СП9 СП18 СП21 СП23 СП24 ПП5 ПП6	СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25		СП3 СП4 СП5 СП8 СП9 СП11 СП12 СП13 СП14 СП15 СП18 СП19 СП22 СП23 СП24 ПП6		СП1 СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП20 СП22 СП23 СП24 ПП5 ПП6	СП1 СП3 СП4 СП5 СП8 СП9 СП10 СП11 СП12 СП14 СП16 СП19 СП20 СП22 СП23 СП24 ПП5 ПП6	СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 СП23 СП24 ПП6	СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП18 СП19 СП22 СП23 ПП6	СП4 СП5 СП8 СП12 СП14 СП18 СП19 СП21 СП22 ПП5 ПП6	

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
									СП26 ПП5 ПП6										
PH20																СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ПП6	СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП18 СП19 СП22 ПП6	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22 СП23 ПП5 ПП6	
PH21									СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 СП26	СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 ПП5 ПП6	СП3 СП4 СП5 СП7 СП11 СП17 СП20 ПП5 ПП6			СП1 СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП20 СП22 СП23 СП24 ПП5 ПП6	СП1 СП3 СП4 СП5 СП8 СП9 СП10 СП11 СП12 СП14 СП16 СП19 СП20 СП22 СП24 ПП5 ПП6	СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ПП6	СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП18 СП19 СП22 ПП6	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22 СП23 ПП5 ПП6	

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
										ПП5 ПП6									
PH22										СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 СП26 ПП5 ПП6	СП1 СП2 СП4 СП5 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП5 ПП6	СП3 СП4 СП5 СП7 СП11 СП17 СП20 ПП5 ПП6			СП1 СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП20 СП22 СП23 СП24 ПП5 ПП6	СП1 СП3 СП4 СП5 СП8 СП9 СП10 СП11 СП12 СП16 СП19 СП20 СП22 СП25 ПП5 ПП6	СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ПП6	СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП18 СП19 СП22 ПП6	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22 СП23 ПП5 ПП6

8. РЕЗУЛЬТАТИ ОБГОВОРЕННЯ ОСВІТНЬОЇ ПРОГРАМИ

Стейкхолдери (вказати ПІБ та посаду, місце роботи)	Зауваження/Рекомендація	Враховано / частково враховано / не враховано	Примітка
Вадим МАШТАЛІР, доктор історичних наук, професор, заслужений винахідник України, начальник інституту інформаційно-комунікаційних технологій та кібероборони	Позитивний відгук. Без зауважень.	-	-
Юрій ПУНДА, доктор військових наук, старший науковий співробітник, начальник навчально-наукового центру підготовки офіцерів багатонаціональних штабів	Позитивний відгук. Без зауважень.	-	-
Валерій ШЕСТАКОВ, доктор технічних наук, доцент, лауреат Державної премії України в галузі науки і техніки, заступник директора (з навчальної та наукової роботи) Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України.	Позитивний відгук. Без зауважень.	-	-
Сергій ГОЛОВАШИЧ, кандидат технічних наук, ТОВ “Мікрокрипт Текнолоджіс”, генеральний директор	Позитивний відгук. Без зауважень.	-	-

Завідувач кафедри кібербезпеки  Сергій ЄВСЕЄВ

Гарант освітньої програми  Роман КОРОЛЬОВ

9. ПЛАН ВРАХУВАННЯ ЗАУВАЖЕНЬ/РЕКОМЕНДАЦІЙ ЗА РЕЗУЛЬТАТАМИ АКРЕДИТАЦІЙНОЇ ЕКСПЕРТИЗИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Рекомендації, надані під час останньої акредитації	Період врахування (короткостроковий/довгостроковий/не доцільно враховувати)	Заходи, що спрямовані на врахування рекомендацій/Обґрунтування щодо недоцільності впровадження рекомендації	Терміни впровадження заходів/відповідальні особи
Загальні рекомендації Експертної групи та Галузевої експертної групи (по кафедрі, галузі, інституту, університету)			
Рекомендація 1			
Рекомендація 2			
Рекомендація 3			

Акредитація планується на 2027 навчальний рік.

Директор навчально-наукового інституту
комп'ютерних наук та інформаційних технологій _____



Михайло ГОДЛЕВСЬКИЙ

Гарант освітньої програми _____



Роман КОРОЛЬОВ